CLAIMS

What is claimed is:

1. A method for secure communications between a client and a server, comprising:

(a) managing a communications negotiation between the client and the server;

(b) receiving encrypted data packets from the client;

(c) decrypting each encrypted packet data;

(d) forwarding unencrypted data packets to the server;

(e) receiving data packets from the server;

(f) encrypting the data packets from the server; and

(g) forwarding encrypted data packets to the client.

2. The method of claim 1 wherein said step of managing comprises:

receiving TCP session negotiation data from the client and modifying the negotiation data prior to forwarding the data to the client.

3. The method of claim 2 wherein the method includes the further step of modifying a SYN request from the client to the server to alter the packet transmission parameters.

4. The method of claim 3 wherein said step of modifying includes modifying at least a maximum segment size value of said data packet.

5. The method of claim 3 wherein the method further includes the steps of negotiating an SSL session with the client.

6. The method of claim 5 wherein the steps (c) and (f) comprise decrypting SSL encrypted packet data, and encrypting a data packet with SSL.

7 The method of claim 1 wherein said step of managing comprises receiving communication negotiation data directed to the server from the client and responding to said negotiation in place of the server.

8. The method of claim 7 wherein further including a step, prior to said step (d), of negotiating a separate TCP session with the server.

9. The method of claim 1 wherein the step of managing comprises receiving communication negotiation data destined for an intermediary device, altering a destination and source IP addresses of the data, and forwarding the data to the server.

10. The method of claim 9 wherein said step of receiving communication data comprises the receiving an ACK packet from said server destined for the intermediary device, altering the packet's destination and source IP addresses, and forwarding the packet to the client.

11. The method of claim 1 further including the step, prior to said step of receiving encrypted data, of negotiating an encrypted data communications session between an intermediary device and the client.

12. The method of claim 1 wherein said step of managing comprises maintaining a database of entries on each session of data packets communicated between the client and the server.

13. The method of claim 12 wherein said database includes an entry for a session comprising a session ID, a TCP Sequence number and an SSL session number.

14. The method of claim 12 wherein said entry further includes an initialization vector.

15. The method of claim 12 wherein said entry includes an expected ACK.

16. The method of claim 1 wherein said step of receiving encrypted data packets includes receiving data packets including encrypted application data spanning multiple packets, and said step of forwarding includes forwarding a portion of the application data contained in an individual encrypted TCP segments to the server without authentication.

17. The method of claim 16 further including the step of authenticating the application data on receipt of all packets including the application data.

18. The method of claim 16 wherein said data is not buffered during decryption.

19. The method of claim 16 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

20. A method for secure communications between a client and one of a plurality of servers performed on an intermediary device, comprising:

(a) establishing a communications session between the client and said one of said plurality of servers by receiving negotiation data from the client intended for the server and forwarding the negotiation data in modified form to the server, and receiving negotiation data from the server intended for the client and forwarding the negotiation data to the client ;

(b) establishing a secure communications session between the client and the intermediary device;

(c) maintaining a database of the secure communications session including information on the session/packet associations;

(d) receiving encrypted application data from the intermediary device;

(e) decrypting the application data; and

(f) forwarding decrypted application data to said one of said plurality of servers.

21. The method of claim 20 further including the steps of:

(h) receiving application data from the server;

(i) encrypting the application data; and

(j) forwarding the application data to the client.

22. The method of claim 20 wherein the method further includes the step of selecting one of the plurality of servers for each packet in the communications session and mapping all communications intended for the server to said one of said plurality of servers.

23. The method of claim 23 wherein the step of managing comprises receiving packets from said one of said plurality of servers and modifying the source and destination addresses of the packet to return the packet to the client.

24. The method of claim 23 wherein said step of decrypting application comprises decrypting data and forwarding said data on to said one of said plurality of servers via a secure network.

25. The method of claim 24 further including the step of receiving application data from said one of said plurality of servers, encrypting said data, and forwarding encrypted data to said client.

26. The method of claim 20 wherein said database includes an entry for a session comprising a session ID, a TCP Sequence number and an SSL session number.

27. The method of claim 20 wherein said entry further includes an initialization vector.

28. The method of claim 20 wherein said entry includes an expected ACK.

29. The method of claim 20 wherein said step of forwarding includes:

forwarding data which spans over multiple TCP segments and forwarding data which is not authenticated.

30. The method of claim 29 wherein said data is not buffered during decryption.

31. The method of claim 29 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

32. The method of claim 29 wherein said step of forwarding includes authenticating the decrypted data after a final segment of a multi-segment encrypted data stream is received.

33. An apparatus coupled to a public network and a secure network, communicating with a client via the public network and communicating with one of a plurality of servers via the secure network, comprising:

a network communications interface;

at least one processor;

programmable dynamic memory;

a communications channel coupling the processor, memory and network communications interface;

a client/server open communications session manager;

a client secure communication session manager;

a client/server secure communications session tracking database; and

a data packet encryption and decryption engine.

34. The apparatus of claim 33 wherein the client open communications session manager and secure communication manager enables the apparatus as a TCP and SSL proxy for the server.

35. The apparatus of claim 33 wherein the communications session managers enable transparent secure and open communication between the client and the server.

36. The apparatus of claim 33 wherein the client negotiation managers route packets between the client and said one of said plurality of servers by modifying source and destination addresses.

37. The apparatus of claim 33 further including a load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers.

38. The apparatus of claim 33 wherein data packet encryption and decryption engine performs SSL encryption and decryption on data packets transmitted between the client and said at least one server.

39. The apparatus of claim 41 wherein the session tracking set maintains database having at least one record per communication session between the client and server.

40. The apparatus of claim 33 wherein said session tracking database includes a TCP sequence number and an SSL sequence number.

41. The apparatus of claim 41 further including a recovery manager coupled to the database.

42. The apparatus of claim 33 wherein said data is not buffered during decryption.

43. The apparatus of claim 33 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

44. The apparatus of claim 43 wherein said decryption instruction set includes an authentication process which authenticates

the decrypted data after a final segment of a multi-segment encrypted data stream is received.

45. An secure sockets layer processing acceleration device, comprising:

a client communication engine establishing a secure communications session with a client device via an open network;

a server communication engine establishing an open communications session with a server via a secure network; and

an encryption and decryption engine operable on encrypted data packets received via the open communications session and on clear data received via the open communications session.

46. The SSL acceleration device of claim 45 wherein the client communication engine forwards modified communication session data to at least one server.

47. The SSL acceleration device of claim 45 wherein the client communication engine acts as a proxy for one or more servers in communication with the SSL acceleration device.

48. The SSL acceleration device of claim 45 further including a session tracking database interacting with the encryption and decryption engine tracking client and server communications.

49. The SSL acceleration device of claim 45 wherein the encryption and decryption engine includes a bufferless mode transmitting decrypted, unauthenticated data to a server.

50. The SSL acceleration device of claim 45 further including a load balancing engine.